ITCS 412: Cryptography
First Semester 2011/2012
Test I

Section :

(1)	2
9:00	12:00

This exam consists of **6** pages. Duration: One hour

	Part 1	Part2	Part 3	Total
Maximum	10	20	10	40
Grade	8	17 ½	9 ½	35

Part 1:

Answer the following questions by clearly circling the most appropriate answer (1 point each)

1. Access Control mechanism
   a. Ensures the identity of an entity
   b. Enforces access rights to resources
   c. Enables the selection of particular physical secure route
   d. Enhances detection of security relevant events

2. Which of the following is not a security mechanism as defined by X.800:
   a. Event Detection
   b. Digital Signature
   c. Traffic padding
   d. Data Confidentiality

3. Implements the security *policies* of the data processing systems and information transfers of an organization
   a. Security functionality
   b. Security mechanism
   c. Security attack
   d. Security service

4. What is the subkey size in each round of DES?
   a. 56 bits
   b. 48 bits
   c. 32 bits
   d. 64 bits

5. Which of the following modes of operation is suitable for bursty traffic, can do parallel decryption of packets, suitable for hardware implementation, and is as secure as the others

a. CTR (Counter Mode)
b. ECB (Electronic Codebook)
c. CFB (Cipher Feedback)
d. OFB (Output Feedback)

6. What is the main component in a Feistel network that is responsible for diffusion

a. The subkeys
b. The swap operation
c. The S-box
d. The initial permutation (IP)

7. The most difficult attack is presented when all that is available

a. Ciphertext only
b. Known plaintext
c. Chosen plaintext
d. Statistical of plaintext

8. A cipher that uses rail fence cipher followed by one-time pad is

a. Autokey cipher
b. Product cipher
c. Substitution cipher
d. Transposition cipher

9. To which stage in AES the avalanche effect can be mainly attributed

a. MixColumn Transformation
b. Addroundkey transformation
c. ByteSubstitution transformation
d. Forward state substitution transformation

10. A cryptographic algorithm uses three keys of size 24, 24 and 21 bits for encryption. On average how long would it take an attacker to break the code using brute force

a. 2^{23}
b. 2^{24}
c. 2^{68}
d. 2^{69}
e. 2^{70}

17½

Part 2:

Q1. In cryptographic systems the type of operations used for transforming plaintext to ciphertext are based on two general principles. **List** and **define** the two principles. [3 points]

a. Transposition is rearrengeing the content of the message without changing or altering any thing. and it use to provide diffison.

b. Subsituation is replacing the letters / bits by another letters / symobls / charaters / to provide confision.

Q2. The number of keys used in symmetric encryption algorithms are 1 key [1 point]

Q3. Write the encryption equation for RSA public key algorithm. [1 point]

$C = M^e \bmod n$

Q4. Briefly explain each of the following attacks: [4 points]

I. Masquerade is someone / some entity pretend claimed to be another one "personate"

II. Replay read the messages, and then retransimmeted / reserved again in order to achive unauthentication effect

III. Denial of service preventing from normal use of Server, managment of communication

IV. Traffic Analysis monitoring the traffic, to see how much data / resource are send or recived in order to know some usefull information

Q5. Construct a playfair matrix with the key **golden** and encrypt the following message **Generaly**. [4 points]

G	O	L	D	E
N	A	B	C	F
H	I/J	K	M	P
Q	R	S	T	U
V	W	X	Y	Z

→ GE NE RA LY

* OG FG WI DX cipherText1

* OG EG WJ DX cipherText2

A 0
B 1
C 2
d 3
E 4
F 5
G 6
H 7
i 8
J 9
K 10
L 11
M 12
N 13
O 14
P 15
Q 16
R 17
S 18
t 19
U 20
V 21
W 22
X 23
Y 24
Z 25

Q6. Consider the following encryption Grids.

Upper Grid	1	2	3	4	5	...	26
Lower Grid	A	B	C	D	E	...	Z

shift

The lower grid can shift its elements and thus the alignment with the upper grid can change (in circular fashion). The upper grid does not move. Assume that the key is the three letter (DPM), then the lower grid shifts the letters until letter D aligns with number 1 in the upper grid; and whatever letter is in the plaintext is encrypted with the letter in the lower grid. The next letter in plaintext is encrypted after aligning the lower grid with letter P aligned with number 1, and the encryption is done. For the third letter in plaintext is encrypted after aligning the lower grid with letter M with number 1. This process is repeated for the next three letters in the plaintext.

(a) What type of encryption algorithm is this (circle one)? [1 point]

i. Monoalphabetic
ii. Polyalphabetic
iii. Product cipher
iv. Block cipher

(b) Given a n letter key, how many different possible keys are there? [1 point]

26^n 2^n

(c) What would be a good policy for breaking it? [2 points]

I think kasiski method will be good way to attacked. which is see if some pattern is repeated in the text. and this will give us a hint about the key size, after knowing the key size, we can use a Brute force Search to get it the key (DPM) FATIMA

Q7. List one advantage and two limitations of Cipher Block Chaining mode - CBC [3 points]

Advantage 3 each block will Linked to the perouse one

Limitations So any changeing in one bit will lead to change many and many other bits, and this will lead to differ (cualanche effect).

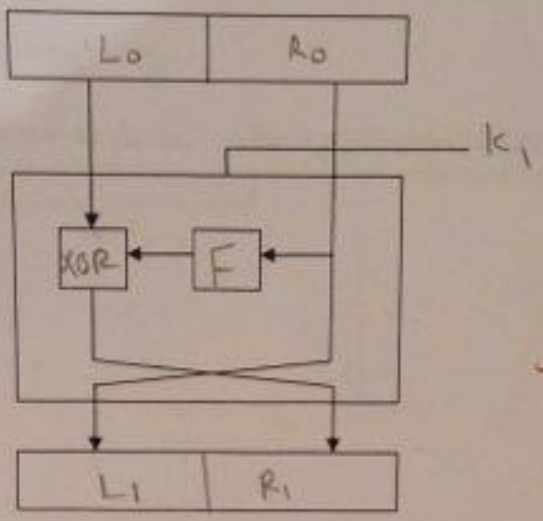
* use the IV which need to distribute it Securely.

* Error profigation: because each block is depending on the previous block, So any Error in one block will achive to another Errors in the blocks after it.

4

Part 3:

Q8. In the following diagram: [4 points]



4

I. Fill in the diagram from the following keywords (L0, R0, F, XOR, L1, R1, K1)

II. Write the equations to produce L_1 and R_1 for one round of DES.

$L_1 = R_0$

$R_1 = L_0 \oplus F(R_0, k_1)$

Q9. AES consists of four stages one of permutation and three of substitution. [3 points]

I. Which stage if removed, the algorithm provides no security. add RoundKey

II. Which stage is mainly responsible for permutation? shiftRow

III. What is the rationale behind the Byte substitution

Here we are using the S-box and this box is resistance for all known attack because of Low correlations between

IV. What is the rationale behind the shiftRow transformation.

As you know; The data is put it into a Matrix, in that Matrix the distribution of the data is done column, by column and in this stage the shifting is done ber row.

So each column will spreed through the raws, so this will lead to change many and many bits more than Excepted " diffusion " Or " Evalanchy effect " is achieved.

3

5

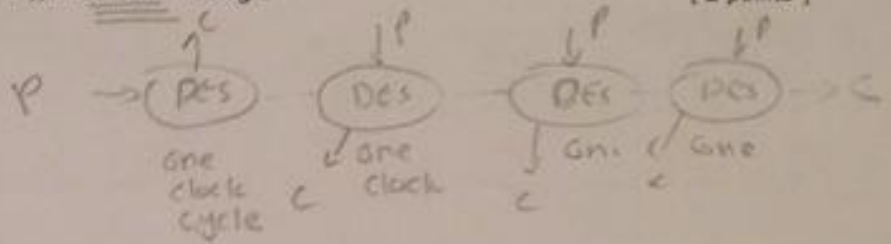
byte Substitution
shiftRow
MixColum
add RoundKey

* access control
* availbilty
* data Integrety
* data confidenty
* non-rep

Q10. TCP protocol is a connected oriented protocol that deals with a stream of messages. However, it does not assure that messages are received as sent with no duplication insertion, modification, reordering or replay. Which of the five security services is needed to assure none of the previous attacks occurred. [1 point]

data Integrity. ✓ 1

Q11. Assume that you have a chip that includes four DES units working in parallel. Each DES unit takes one clock cycle to complete one encryption. How many clock cycles are needed using one of these chips to encrypt a 512-bit message? [2 points]



512 bit of message

64

512 bits

DES => size of block 64 bit

1 1/2

* number of blocks = 512/64 = 8 blocks

8 block = 8 x 1 = 8/4 clock cycles = 2 clock cycles

each Encryption will Encrypt two block

4 (2) x1 = 8